CLAIMS:

1. A method of verifying the authenticity of media content, said method comprising the steps of:

extracting a sequence of first authentication bits from said media content by comparing a property of the media content in successive sections of the media content with a second threshold,

receiving a sequence of second authentication bits, said received sequence being extracted from an original version of the media content by comparing said property of the media content with a first threshold, and

declaring the media content authentic if the received sequence of second authentication bits matches the extracted sequence of first authentication bits,

characterised in that the step of extracting the authentication bits from the media content comprises setting the second threshold in dependence upon the received authentication bits, such that the probability of an extracted authentication bit in said sequence of first authentication bits mismatching the corresponding received authentication bit in said sequence of second authentication bits is reduced compared with using the first threshold for said extraction.

2. The method according to claim 1, wherein the false alarm rate when verifying authenticity of said media content is reduced.

3. The method according to any of claims 1 or 2, wherein the step of extracting the authentication bits from the media content comprises controlling the threshold in dependence upon the received authentication bits such that the probability that an extracted authentication bit matches the corresponding received authentication bit is high.

4. The method according to any of claims 1 to 3 further comprising controlling the second threshold during the step of extracting the authentication bits based upon the current mismatching authentication bits, in such a manner that the authenticity decision

process is adjusted according to previously thus far discovered mismatching authentication bits, leading to improved localisation of non-authentic section(s) in said media content.

5. The method according to any of claims 1 to 4, comprising declaring the media content as a whole tampered with, if the received sequence of second authentication bits does not match the extracted sequence of first authentication bits.

6. The method according to claim 5, wherein mis-matching bits between the received sequence of second authentication bits and the extracted sequence of first authentication bits comprise information on localisation of at least a first section in said media content, said method further comprising the step of

identifying and/or marking the localisation of tampered sections in said media content for visualisation of at least one tampered section(s).

7. The method according to claim 6, further comprising subsequent phases in which the step of extracting is repeated using a modified second threshold.

8. The method according to claim 7, wherein said step of extracting is solely executed on sections of said media content neighbouring to sections of said media content being identified as tampered.

9. A method as claimed in claim 1, comprising further phases in which the step of extracting is repeated, the second threshold being controlled in dependence upon the distance between the section for which the authentication bit is extracted and sections for which it has been found that the authentication bits mismatch the received authentication bits.

10. The method according to claim 1, wherein the segments are blocks and the media content is a digital image,

wherein the step of extracting comprises making an authentication decision for each block independently and the second threshold is firstly derived from a low false alarm operating point,

wherein the step of declaring comprises declaring the image as authentic if no blocks are declared tampered or declaring the image as a whole being inauthentic if at least one tampered blocks are found,

wherein blocks neighbouring those that are tampered are declared having a higher probability of being tampered than non-neighbouring blocks, and new operating points are selected for remaining blocks, not being declared tampered in previous runs, for repeated authentication decisions until no further tampered blocks are identified.

11. The method according to claim 10, further using alterations to the decision boundary to move the operating point to a position with a larger detection probability.

12. The method according to any of claims 10 or 11, further comprising determining the full size and shape of a tampered image region by marking of tampered blocks in the image.

13. The method according to claim 1, wherein said adjusting of said second threshold comprises adjusting the operating point or the decision boundary or prior probabilities according to context information as given by a neighbouring decision.

14. The method according to any of the preceding claims, wherein the second threshold is adjusted according to the formula:

$$\lambda_i = \alpha\lambda_1 + (1-\alpha)\lambda_2,$$

wherein $\lambda_1 = 1$ and $\lambda_2 > 1$ are decision thresholds, and α is given by:

$$\alpha = \left(\frac{n}{m}\right)\left(\frac{d - r_m}{d-1}\right), \text{ and } r_m = \min(r, d),$$

wherein n is the number of blocks neighbouring block i that are marked as tampered, m is the total number of blocks neighbouring block i, r is the distance in units of blocks of block i from the closest tampered block, and d is the maximum distance that sets how widely around a tampered block that suspicion is raised,

wherein a subsequent authentication decision is re-evaluated using the new second threshold λ_i, and

if further blocks are declared tampered in the subsequent authentication decision, the procedure of adjusting the second threshold and re-evaluating blocks' authenticity is repeated until no further tampered blocks are identified.

15. The method to any of the preceding claims, wherein the second threshold used to determine the authentication bits represents an operation point on a ROC curve.

16. Application of the method according to claim 1 in multimedia authentication decisions, wherein said multimedia comprises image or video and/or audio data.

17. Application according to claim16, wherein said multimedia authentication decisions are applied in surveillance systems.

18. Application according to any of claims 16 or 17, wherein adjustment of a decision boundary in multimedia authentication decisions is based on context information.

19. Application according to claim 18, wherein said context information is based on proximity to areas already determined as tampered during tampering localisation of said multimedia.

20. A device (8) for verifying the authenticity of media content by performing the method according to claim 1, said device comprising

means (80) for extracting a sequence of first authentication bits from said media content by comparing a property of the media content in successive sections of the media content with a second threshold,

means (81) for receiving a sequence of second authentication bits, said received sequence being extracted from an original version of the media content by comparing said property of the media content with a first threshold, and

means (82) for declaring the media content authentic if the received sequence of second authentication bits matches the extracted sequence of first authentication bits,

characterised in that the means for extracting the authentication bits from the media content comprises means (83) for setting the second threshold in dependence upon the received authentication bits, such that the probability of an extracted authentication bit in said sequence of first authentication bits mismatching the corresponding received authentication bit in said sequence of second authentication bits is reduced compared with using the first threshold for said extraction.

21. A computer-readable medium (9) having embodied thereon a computer program for verifying the authenticity of media content by performing the method according to claim 1, and for processing by a computer (94), the computer program comprising

a first code segment (90) for extracting a sequence of first authentication bits from said media content by comparing a property of the media content in successive sections of the media content with a second threshold,

a second code segment (91) for receiving a sequence of second authentication bits, said received sequence being extracted from an original version of the media content by comparing said property of the media content with a first threshold, and

a third code segment (92) for declaring the media content authentic if the received sequence of second authentication bits matches the extracted sequence of first authentication bits,

characterised in that the code segment (90) for extracting the authentication bits from the media content comprises a code segment (93) for setting the second threshold in dependence upon the received authentication bits, such that the probability of an extracted authentication bit in said sequence of first authentication bits mismatching the corresponding received authentication bit in said sequence of second authentication bits is reduced compared with using the first threshold for said extraction.